Amendments to the Claims:

Please amend claim 30 as set forth below. A complete listing of pending claims is provided below. The Examiner is respectfully requested to enter claim 30 as amended. The listing of claims below should replace all previously amended claims in this application. No new matter has been added.

Listing of Claims:

1. (Previously presented) A method, comprising:

obtaining a hint;

obtaining a password;

performing a hashing algorithm on the hint and the password to generate a key;

encrypting data using the key;

sending the encrypted data to a server for storage; and

sending the hint to a client.

2. (Original) The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password.

3. (Previously presented) A method, comprising:

obtaining a hint;

obtaining a password;

performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key;

encrypting data using the key; and

sending the encrypted data to a server for storage.

4. (Previously presented) A system, comprising:

a user interface for obtaining a password;

a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key;

an encryption engine coupled to the key generator for encrypting data using the key;

a communications module coupled to the engine for sending the encrypted data and the hint to a server for storage.

5. (Original) The system of claim 4, further comprising a hint generator for generating the hint.

6. (Original) The system of claim 4, wherein the key generator hashes the password.

7. (Previously presented) A system, comprising:

a user interface for obtaining a password;

a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator hashes the password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key;

an encryption engine coupled to the key generator for encrypting data using the key; and

a communications module coupled to the engine for sending the encrypted data to a server for storage.

8. (Previously presented) A system, comprising:

means for obtaining a hint;

means for obtaining a password;

means for performing a hashing algorithm on the hint and the password to generate a key;

means for encrypting data using the key;

means for sending the encrypted data to a server for storage; and

means for sending the hint to a client.

9. (Original) The system of claim 8, wherein the system includes code stored on a computer-readable storage medium.

10. (Original) The system of claim 8, wherein the system includes code embodied in a carrier wave.

11. (Original) A method, comprising:

receiving a request to store encrypted data from a client;

sending a request to store encrypted data from a client;

sending an encryption downloadable for deriving a key to encrypt data to the client;

receiving encrypted data that was encrypted by the encryption downloadable from the client; and

obtaining a hint, corresponding to the encrypted data and needed for regenerating the key; and

storing the hint and the encrypted data.

12. (Original) A system, comprising:

an encryption downloadable for deriving an encryption key from a password and a hint;

a web server for interfacing with a client, for sending the encryption downloadable to the client, and for receiving encrypted data that was encrypted by the encryption downloadable from the client; and

memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data.

13. (Previously presented) A method, comprising;

obtaining a password;

sending encrypted data and a hint corresponding to the encrypted data from a server to a client; and

performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data.

14. (Original) The method of claim 13, wherein the step of performing a hashing algorithm includes hashing the password.

15. (Previously presented) a system, comprising:

a user interface for obtaining a password;

a communication module for sending encrypted data and a hint corresponding to the encrypted data from a server to a client; and

a key generator for performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data.

16. (Previously presented) A system, comprising:

means for obtaining a password;

means for sending encrypted data and a hint corresponding to the encrypted data from a server to a client; and

means for performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data.

17. (Original) The system of claim 16, wherein the system includes code stored on a computer-readable storage medium.

18. (Original) The system of claim 16, wherein the system includes code embodied in a carrier wave.

19. (Previously presented) A method, comprising:

receiving identification of encrypted data;

sending a decryption downloadable for deriving a key from a password and a hint to a client;

sending a hint corresponding to the encrypted data to the client; and

deriving the key by hashing at least one of the hint and the password.

20. (Previously presented) A system, comprising:

a decryption downloadable for deriving a key by hashing at least one of a password and a hint;

encrypted data;

a hint corresponding to the encrypted data; and

a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client.

21. (Original) A client based method, comprising:

obtaining a password;

deriving a first secret from the password;

receiving a hint corresponding to data to be decrypted from a server;

deriving an intermediate index from the first secret and the hint; and

sending the intermediate index to the server.

22. (Original) The method of claim 21, wherein deriving the first secret includes hashing the password.

23. (Original) The method of claim 21, wherein deriving an intermediate index includes

hashing the first secret and the hint.

24. (Original) A system, comprising:

a user interface for obtaining a password;

an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password; and

a communications engine coupled to the index generator for sending the intermediate index to the server.

25. (Original) The system of claim 24, wherein the index generator generate the intermediate index by hashing the hint and the secret.

26. (Original) A system, comprising;

means for obtaining a password;

means for deriving a first secret from the password;

means for receiving a hint corresponding to data to be decrypted from a server;

means for deriving an intermediate index from the first secret and the hint; and

means for sending the intermediate index to the server.

27. (Original) The system of claim 26, wherein the system includes code stored on a computer-readable storage medium.

28. (Original) The system of claim 26, wherein the system includes code embodied in a carrier wave.

29. (Original) A server-based method, comprising;

receiving an indication of encrypted data to be decrypted;

transmitting to a client a hint corresponding to the indication, and a decryption downloadable for deriving an intermediate index from a password and the hint;

receiving the intermediate index from the client; and

deriving a decryption key from a second secret corresponding to the user and the intermediate index.

30. (Currently Amended) A system, comprising;

a second secret corresponding to a user;

a decryption downloadable for generating an intermediate index from a password and a hint;

a web server for receiving an indication of encrypted data to be decrypted, for transmitting the decryption downloadable and a hint corresponding to the indication to a client, and for receiving an intermediate index from the[e] client; and

a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index.

REMARKS

Claims 1-30 remain pending in the above identified application. Claim 30 has been amended to correct a typographical error. No new matter has been added.

Claim rejections - 35 U.S.C. § 112

Claims 19 and 20 have been rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps. The Office Action states the omitted step is the step for "deriving a key." Applicant respectfully traverses this rejection. Claim 19 recites "deriving the key by hashing at least one of the hint and the password." Thus, the key is derived by "hashing at least one of the hint and the password." Claim 20, recites a system, as such, the claim recites components operable to perform a method as opposed to the method itself. Applicant therefore submits that claims 19 and 20 satisfy the requirements of 35 U.S.C. 112, second paragraph and withdrawal of the rejection is respectfully requested.

Claim Objection

Claim 30 has been objected to because of a typographical error that resulted in a misspelling. Claim 30 has been amended to properly spell the word "the." Applicant submits this correction removes the informality and respectfully requests withdrawal of the objection.

Claim rejections - 35 U.S.C. § 102(e)

Claims 1 -2, 4-6, and 8-19 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,360,322 to Grawrock ("Grawrock"). Claims 3, 7, and 20-30 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated U.S. Patent No. 6,470,454 to Challener et al. ("Challener"). Applicant respectfully traverses these rejections as hereinafter set forth.

A claim is anticipated only if each and every element as set forth in the claim is found either expressly or inherently described in a single prior art reference. *Verdegaal Brothers v Union Oil Co.*

of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claims 1 and 8 recite, inter alia, "performing a hashing algorithm on the hint and the password to generate a key." At a minimum, Applicant respectfully submits that Grawrock does not disclose this element. The Office Action cites col.6 line 52 to col. 7 line 27 of Grawrock as disclosing this element. The cited passages however do not disclose this element, rather Grawrock discloses only hashing a user entered password. (col. 6 lines 52-55). Therefore the reference does not anticipate these claims.

Claim 4 recites, inter alia, "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key." As discussed above, at a minimum, Applicant respectfully submits that Grawrock does not disclose this element. The Office Action cites col.6 line 52 to col. 7 line 27 of Grawrock as disclosing this element. The cited passages however do not disclose this element but rather disclose only hashing a user entered password. (col. 6 lines 52-55). Therefore the reference does not anticipate this claim.

With respect to claim 11, the Office Action states that Grawrock "suggests receiving a request to store encrypted data from a client." Applicant respectfully submits that Grawrock does not disclose or suggest this element. The Office Action cites col. 2 lines 54-62 of Grawrock as disclosing this element. The cited passage however does not disclose this element but rather discloses a one time password mechanism which is an instruction set. (col. 2, lines 47-54) Therefore the reference does not anticipate claim 11.

Claim 12 recites, *inter alia,* "memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data." Applicant respectfully submits that Grawrock does not disclose this element. The Office Action cites col. 5 lines 1-42 as disclosing this element. The cited passages however do not disclose this element, but rather disclose an authenticating entity (col. 5, lines 29-42). Therefore, the reference does not anticipate this claim.

Claims 13, 15 and 16 recite, inter alia, "performing a hashing algorithm on the password and the hint at the client to generate a key." At a minimum, Applicant respectfully submits that Grawrock does not disclose this element. The Office Action cites col.6 line 52 to col. 7 line 27 of

Grawrock as disclosing this element. The cited passages however do not disclose this element rather Grawrock only discloses hashing a user entered password. (col. 6 lines 52-55). Therefore the reference does not anticipate these claims.

Claim 19 recites, inter alia, "receiving identification of encrypted data." At a minimum, Grawrock does not disclose this element. The Office Action cites col. 2 lines 54-62 as disclosing this element. The cited passage does not disclose this element, specifically; this passage provides a brief description of a data processing system. (col. 2 line 62). Therefore the reference does not anticipate this claim.

Based on at least the reasons noted above, Applicant respectfully submits that claims 1, 4, 8, 11, 12, 13, 15, 16, and 19 are not anticipated by Grawrock. Given that claim 2 depends from claim 1, claims 5-6 depend from claim 4, claims 9-10 depend from claim 8, claim 14 depends from claim 13, and claims 17-18 depend from claim 16, accordingly, it is respectfully submitted that these claims are not anticipated by Grawrock for at least the same reasons.

Claim 3 recites, inter alia, "performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key." At a minimum, Applicant respectfully submits that Challener does not disclose this element. The Office Action cites col. 5, lines 51-58 of Challener as disclosing "performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret" The cited passage however, does not disclose this element, rather, this passage discloses text input which is preferably a combination of the serial number of the data processing system and the enterprise key, not a hint or a password. Moreover, the cited passage of Challener produces as an output a hash value which is processed to develop a password as opposed to a key as recited in claim 3. Finally, Challener recites entering a "relatively-secret key" (col. 6, lines 6-7) as oppose to "deriving a first secret" from the hashed password as recited in claim 3. Thus, for at least these reasons the reference does not anticipated claim 3.

Claim 7 recites, inter alia, "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator hashed the password to derive a first secret." At a minimum, Applicant respectfully submits that Challener does not disclose this element. The Office Action cites col. 5, lines 51-58 of Challener as disclosing this element. The cited passage however, does not disclose this element, rather, this passage discloses text input which is preferably a combination of the serial number of the data processing system and the enterprise key, not a hint or a password. Moreover, the cited passage of Challener produces as an output a hash value which is processed to develop a password as opposed to a key as recited in claim 7. Therefore the reference does not anticipated claim 7.

Claims 20, 21, and 26 recite, inter alia, "deriving an intermediate index from the first secret and the hint." At a minimum, Applicant respectfully submits that Challener does not disclose this element. The Office Action cites col. 5, line 59- col. 6 line 33 of Challener as disclosing this element. The cited passage however, does not disclose this element, rather, this passage discloses text input which is preferably a combination of the serial number of the data processing system and the enterprise key, to generate a password. In claims 20, 21 and 26, the first secret and the hint are used to generate the intermediate index (Specification, p. 15) Therefore the reference does not anticipated claim 20, 21, and 26.

Claim 24 recites, inter alia, "an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password." At a minimum, Applicant respectfully submits that Challener does not disclose this element. The Office Action cites col. 5, line 59 - col. 6 line 33 of Challener as disclosing this element. As discussed with respect to claims 20, 21 and 26, the cited passage discloses text input which is preferably a combination of the serial number of the data processing system and the enterprise key, to generate a password. Challener does not disclose the use of a hint and a secret to generate an intermediate index. Therefore the reference does not anticipated claim 24.

Claims 29 and 30 recite, inter alia, "a decryption downloadable for generating an intermediate index from a password and a hint." At a minimum, Applicant respectfully submits that Challener does not disclose this element. The Office Action cites col. 6, lines 21-57 of Challener as disclosing this element. The cited passage discloses generating user friendly and uniformly formatted passwords (col. 6, lines 34-36) using an accumulator and a counter. Challener does not disclose the use of a password and a hint to generate an intermediate index. Therefore the reference does not anticipated claims 29 and 30.

Based on at least the reasons noted above, Applicant respectfully submits that claims 3, 7, 20, 21, 24, 26 and 29 are not anticipated by Challener. Given that claims 22-23 depend from claim 21, claim 25 depends from claim 24, and claims 27-28 depend from claim 26 correspondingly, it is respectfully submitted that these claims are not anticipated by Challener for at least the same reasons.